Module 4: Information Security Risks
Best Practices

1	Risk is a measure of the impact of a threat acting on a vulnerable asset.
2	Ensure that your important data is backed up regularly and can be restored when necessary, (and test the backups regularly).
3	Treat everyone with respect to reduce some sources of stress that can create insider threats. Report suspicious behavior to your management.
4	Supervisors and CORs are responsible for ensuring that all computer and building access are removed immediately after an individual no longer works for DOI.
5	Keep in mind that organizations shouldn't request personal information via e-mail. If in doubt, give them a call (but don't use the phone number contained in the e-mail—that's usually phony as well).
7	Never follow a link to a secure site from an e-mail—always enter the URL manually.
8	Don't be fooled (especially today) by the latest scams. Visit the Internet Crime Complaint Center (IC3) and http://www.ic3.gov/crimeschemes.aspx websites for tips and information.
9	Open e-mails from only familiar sources and only navigate to trusted sites.
10	Delete Spam without replying.
11	Do not forward chain letters or Reply All unnecessarily.
12	Be alert for tailgating or piggybacking. Report unauthorized access attempts to the security guard on duty or to facilities management personnel.
13	Comply with facility-defined visitor sign-in and badge requirements. Escort visitors.
14	Secure physical forms of data (paper, screen visibility, CDs, DVDs).
15	Lock areas containing sensitive data or equipment when unattended.
16	Secure sensitive data and dispose of it properly when it is no longer needed.
17	Safeguard building, office, and desk keys.
18	Report lost ID badges or keys immediately.
19	Immediately forward suspected phishing emails to doicirc@ios.doi.gov
20	Stop, and Think before you Connect!
21	Use the Windows key + <L> or <Ctrl> + <Alt> + <Delete> and then <ENTER> to lock the screensaver on your computer whenever you leave your work area, even if it is only for a few minutes.
22	To get rid of a persistent pop-up with a botnet warning scam (or similar), invoke the Start Task Manager from <Ctrl> + <Alt> + <Delete>, select the browser Task in the Applications tab and click on End Task.